

Podmienky spracovania osobných údajov

v zmysle ustanovenia 18/2018 Z.z. - Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov, a podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a o voľnom pohybe týchto údajov a o zrušení smernice 95/46/ES (všeobecné nariadenie o ochrane osobných údajov) („GDPR“)

Osobným údajom sa na účely tohto dokumentu rozumie akákoľvek informácia týkajúca sa určeného alebo určiteľného subjektu údajov. Subjekt údajov sa považuje za určený alebo určiteľný, ak je možné priamo alebo nepriamo identifikovať najmä na základe čísla, kódu alebo jedného alebo viacerých prvkov špecifických pre jeho fyzickú, fyziologickú, psychickú, ekonomickú, kultúrnu alebo sociálnu identitu.

Subjektom údajov sa rozumie fyzická osoba, ku ktorej sa osobné údaje vzťahujú, teda používatelia služby Sledy.

Za **používateľa** služby Sledy sa považuje každá osoba, ktorá si vytvorí užívateľský či firemný účet. Užívateľ služby Sledy prehlasuje, že si je vedomý svojej role **Správca osobných údajov**, ako aj práv a povinností, ktoré z tejto role plynú. Udeľuje výslovný informovaný súhlas **Spracovateľovi** s týmito Zásadami ochrany osobných údajov

Spracovateľom osobných údajov je spoločnosť KMB group s.r.o., Piešťanská 3, 831 02 Bratislava, IČO 47 425 288, spoločnosť zapísaná v obchodnom registri vedenom na Okresnom súde Bratislava I, oddiel Sro, vložka 92152/B (ďalej len ako Spoločnosť). Spoločnosť môže správu a spracovanie osobných údajov zveriť tretej strane za účelom prevádzkovania a správy služby Sledy.

1. Vymedzenie spracovávaných osobných údajov

1.1. Spracovateľ pre Správca na základe Zmluvy spracováva osobné údaje v uvedenom rozsahu:

Účel spracovania	Rozsah osobných údajov	Zvláštna kategória osobných údajov	Kategória subjektov údajov
Vedenie personálnej agendy	Meno a priezvisko fyzickej osoby; dátum narodenia fyzickej osoby, pohlavie, pracovné pozície, interné zamestnanecké číslo, pracovné a/alebo súkromné mobilné a/alebo pevné telefónne číslo; pracovný a/alebo súkromný e-mail; fotografie; dátum nástupu do spoločnosti, dátum odchodu zo spoločnosti, typ úväzku a typ pracovnoprávneho vzťahu, adresu trvalého bydliska, kontaktnú adresu, kontakt pre prípad núdze, informácie o povinných zrážkach zo mzdy, bankové spojenie.	nie	zamestnanci

Účel spracovania	Rozsah osobných údajov	Zvláštna kategória osobných údajov	Kategória subjektov údajov
Vedenie agendy dovoleniek a ďalších typov absencie	Termíny čerpania udalostí absencie (dovolenka, sick days, benefit days, atď. – ďalšie udalosti podľa nastavenia systému zamestnávateľom)	Nie	zamestnanci
Plánovanie smien, plánovanie pracovných činností	Termíny výkonu pracovných činností na základe definície činností zamestnávateľom (napr. práca v kancelárii, práca u klienta, atď.)	Nie	zamestnanci
Evidencia dochádzky zamestnancov	Evidencia odpracovanej doby zamestnanca v rámci jeho pracovných dní.	Nie	zamestnanci
Profil zamestnanca	Okrem identifikačných údajov zamestnanca môže zamestnanec vkladať aj svoje podobizne.	Nie	zamestnanci
Užívateľská a aplikačná podpora	Údaje uložené v aplikácii Schedy	Nie	zamestnanci

- 1.2. Spracovateľ bude osobné údaje podľa tejto Zmluvy spracovávať v elektronickej podobe
- 1.3. Spracovateľ sa zaväzuje Osobné údaje spracovávať s odbornou starostlivosťou.

2. Samostatnosť spracovateľa a pokyny správcu

- 2.1. Spracovateľ bude Osobné údaje spracovávať samostatne pre dosiahnutie stanoveného účelu spracovania v zmysle článku 1.1. a s vynaložením odbornej starostlivosti samostatne rozhodovať o vykonaní jednotlivých úkonov v rámci spracovania osobných údajov, ktoré je potrebné v súlade s platnými právnymi predpismi vykonať.
- 2.2. V prípade, že Spracovateľ od Správcu dostane Pokyn, je ním viazaný.
- 2.3. Pokyny na spracovanie osobných údajov môže za Správcu oznamovať a za Spracovateľa prijímať iba Oprávnená osoba, a to v písomnej (elektronickej) forme.
- 2.4. Spracovateľa nezaväzujú pokyny Správcu, ktoré sú:
 - 2.4.1. urobené inou ako Oprávnenou osobou a adresované inej ako Oprávnenej osobe,
 - 2.4.2. urobené v inej než písomnej (elektronickej) forme,
 - 2.4.3. v rozpore s platnými právnymi predpismi.
- 2.5. Pokiaľ nastane akýkoľvek prípad, keď Spracovateľ nie je pokynom Správcu viazaný, je o takej skutočnosti Spracovateľ povinný Správcu bez zbytočného odkladu informovať.

3. Ukladanie a zabezpečenie osobných údajov

- 3.1. Spracovateľ sa zaväzuje, že bude Osobné údaje uchovávať a spracovávať bezpečne a bude používať všetky primerané bezpečnostné systémy a postupy obvyklé pre spracovanie Osobných údajov.
- 3.2. Spracovateľ sa zaväzuje brániť, prípadne podniknúť všetky možné kroky k zamedzeniu neoprávnenému prístupu, kopírovaniu, úprave, ukladaniu, reprodukcii, zverejneniu alebo distribúcii Osobných údajov.
- 3.3. Pokiaľ Spracovateľ v súvislosti s poskytovaním Služieb využíva Zabezpečovacie prvky, je povinný o Zabezpečovacích prvkoch zachovávať dôvernoscť, nie je oprávnený ich zdieľať s tretími osobami, prevádzať alebo inak zneužívať.
- 3.4. Spracovateľ vytvára záložné kópie databáz (týždenná záloha databázy), ukladáme posledné 4 zálohy. Obnova dát zo zálohy je spolplatnená čiastkou 500€.
- 3.5. V prípade, že ktorákoľvek zo Strán zistí, že:
 - 3.5.1. došlo k neoprávnenému či nezákonnému spracovaniu Osobných údajov;
 - 3.5.2. došlo k strate, poškodeniu alebo zničeniu či inému spôsobu znehodnotenia Osobných údajov;
 - 3.5.3. nastal prípad Narušenia zabezpečenia;
 - 3.5.4. tretia osoba získala neoprávnený prístup k niektorému zo Zabezpečovacích prvkov;je povinná toto bez zbytočného odkladu oznámiť druhej Strane a poskytnúť maximálnu súčinnosť na nápravu.
- 3.6. Pri poskytovaní kvalitných služieb Schedy nám pomáhajú spracovatelia, ktorí pracujú v súlade s európskymi štandardmi ochrany osobných údajov. Spracovávanie osobných údajov týmito tretími stranami je upravené ich vlastnými podmienkami poskytovania služieb. Popis účelov spracovania:
 - 3.6.1. Služba MailChimp a Mandrill na zasielanie hromadných oznámení a notifikácií. Osobné údaje spoločnosti MailChimp sú odovzdávané do USA, pričom spoločnosť MailChimp spĺňa podmienky EU-U.S. Privacy Shield.
 - 3.6.2. Služby štatistiky Google Analytics a Google Tag Manager (<https://policies.google.com/privacy/partners?hl=en>).

4. Vyhlásenie

- 4.1. Spracovateľ vyhlasuje a Správcom zaručuje, že
 - 4.1.1. spĺňa všetky zákonné povinnosti, ktoré pre neho z GDPR a iných právnych predpisov vyplývajú;
 - 4.1.2. bude po celú dobu trvania Zmluvy spracovávať osobné údaje pre Správca v súlade s Slovenským právnym poriadkom, najmä v súlade s GDPR;
 - 4.1.3. bude po celú dobu trvania Zmluvy viesť riadne záznamy o činnostiach spracovania Osobných údajov v zmysle čl. 30 GDPR;
 - 4.1.4. bude podľa tejto Zmluvy spracovávať vo vzťahu k vymedzeným subjektom údajov iba osobné údaje v rozsahu a na účel stanovený Správcom alebo v súlade s účelom tejto Zmluvy;
 - 4.1.5. bude Osobné údaje spracovávať vždy na základe platného právneho titulu, pokiaľ je súčasťou Služieb zhromažďovanie Osobných údajov Spracovateľom;
 - 4.1.6. bude podľa tejto Zmluvy spracovávať presné Osobné údaje a pravidelne ich bude aktualizovať. Osobné údaje, ktoré sú nepresné s prihliadnutím na účely, na ktoré sa spracovávajú, Spracovateľ zmaže alebo opraví po predchádzajúcom Pkyne Správca;

- 4.1.7. bude Osobné údaje ukladať po nevyhnutne potrebný čas podľa Pokynu Správcu.
Spracovateľ sa zaväzuje vykonávať pravidelne kontrolu lehôt na likvidáciu osobných údajov a zabezpečovať likvidáciu osobných údajov, pokiaľ sú na to splnené podmienky;
- 4.1.8. je schopný zaručiť, že sa nebude pri spracovaní osobných údajov pre Správcu správať tak, aby došlo k zníženiu úrovne ochrany osobných údajov zaistenej týmto predpisom.

4.2. Správca vyhlasuje a Spracovateľovi zaručuje, že:

- 4.2.1. v dobe odovzdania Osobných údajov sú Osobné údaje aktuálne a existuje platný zákonný titul pre ich spracovanie;
- 4.2.2. nie je si vedomý žiadneho rizika porušenia platných právnych predpisov v súvislosti s doterajším spracovaním Osobných údajov.
- 4.2.3. súhlasí s umožnením ďalšieho spracovania osobných údajov ďalšími spracovateľmi, ktorí sa zaviazu k ochrane osobných údajov v minimálnom rozsahu, ktorý je stanovený touto zmluvou. V rovnakom rozsahu čo do účelu spracovania a v minimálnom rozsahu, čo do zaistenia bezpečnosti spracovania spracovávaných osobných údajov.

5. Súčinnosť

- 5.1. Súčinnosť pri plnení správcomi povinnosti reagovať na žiadosti o výkon práv subjektov údajov.
- 5.2. Spracovateľ sa zaväzuje poskytnúť Správcomi potrebnú súčinnosť, ktorú od neho možno spravodlivo požadovať, najmä pri:
- 5.2.1. zavádzanie a udržiavanie vhodných technických a organizačných opatrení na zabezpečenie osobných údajov;
- 5.2.2. ohlasovanie prípadov Narušenia zabezpečenia;
- 5.2.3. posudzovanie vplyvu spracovania na ochranu osobných údajov, pokiaľ Správca rozhodne, že je posúdenie vplyvu spracovania v zmysle článku 35 GDPR nevyhnutné vykonať;
- 5.2.4. plnenie povinností predchádzajúcej konzultácie s Úradom na ochranu osobných údajov v zmysle čl.36 GDPR pri vzniku zákonných podmienok.
- 5.3. Spracovateľ sa zaväzuje na výzvu Správcu poskytnúť v stanovenej lehote, ktorá nesmie byť kratšia ako tridsať (30) pracovných dní nevyhnutné informácie potrebné na doloženie, že spracovanie osobných údajov podľa Zmluvy je vykonávané v súlade s platnými právnymi predpismi.
- 5.4. Spracovateľ sa zaväzuje umožniť Správcomi a jeho zástupcom na jeho výzvu v primeranej lehote, ktorá nesmie byť kratšia ako tridsať (30) pracovných dní:
- 5.4.1. prístup k záznamom o činnostiach spracovania Osobných údajov;
- 5.4.2. vykonať kontrolu technických a organizačných bezpečnostných opatrení Osobných údajov;

6. Doba trvania spracovania

- 6.1. Strany sa dohodli, že Spracovateľ bude spracovávať osobné údaje podľa tejto Zmluvy na dobu určitú po dobu trvania zmluvy o užívaní internetovej služby Sledy.
- 6.2. Po ukončení tejto zmluvy si Spracovateľ vyhradzuje právo celý účet Správcu nenávratne vymazať, a to vrátane všetkých existujúcich kópií osobných údajov.

7. Mlčanlivosť

- 7.1. Zmluvné strany prehlasujú, že všetky údaje, informácie a skutočnosti súvisiace s touto Zmluvou a jej plnením a poskytovaním služieb na základe tejto Zmluvy, najmä spracovávané

osobné údaje podľa Zmluvy, vrátane obsahu Zmluvy (s výnimkou informácií, ktoré sú alebo sa stanú verejne známymi inak než porušením tejto Zmluvy a informácií, ktoré príslušná strana mala vo svojom držaní už pred ich obdržaním od druhej zmluvnej strany), sú dôvernými informáciami („Dôverné informácie“). Strany sa zaväzujú, že Dôverné informácie neposkytnú tretej strane a nepoužijú ich na iný účel ako na plnenie tejto Zmluvy, s výnimkou:

- 7.1.1. svojich poradcov viazaných povinnosťou mlčanlivosti v rovnakom rozsahu ako Strany, alebo
 - 7.1.2. príslušných štátnych a iných správnych úradov a súdov, pokiaľ sú strany povinné podľa všeobecne záväzných predpisov im tieto informácie poskytnúť, alebo
 - 7.1.3. informácií, ktoré sú alebo sa stanú verejne dostupnými inak ako porušením tejto Zmluvy.
- 7.2. Spracovateľ sa zaväzuje k povinnosti mlčanlivosti v rozsahu tohto článku Zmluvy zaviazat' svojich zamestnancov a iných spolupracovníkov v zmluvnom vzťahu so Spracovateľom, ktorí vykonávajú činnosti súvisiace s touto Zmluvou a jej plnením a poskytovaním služieb na základe tejto Zmluvy.
- 7.3. Povinnosť mlčanlivosti podľa tejto Zmluvy trvá aj po zániku tejto Zmluvy. Strany nie sú oprávnené po skončení Zmluvy dôverné informácie v zmysle tejto Zmluvy akýmkoľvek spôsobom rozširovať či využiť či umožniť ich šírenie či využitie.

8. Otázky týkajúce sa ochrany osobných údajov

- 8.1. Ak máte nejaké otázky alebo pripomienky týkajúce sa spracovania osobných údajov Spoločnosti, kontaktujte nás.

Posledná aktualizácia dňa 01.01.2022

9. Zoznam prijatých technických a organizačných opatrení na ochranu osobných údajov

- 9.1. Aplikácie aj užívateľské dáta sú umiestnené na serveroch spoločnosti Websupport.
- 9.2. Všetky prístupy k aplikácii sú zabezpečené proti odpočúvaniu pomocou protokolu https a platného šifrovacieho certifikátu.
- 9.3. Priamy prístup k administrácii servera je umožnený iba cez kryptované rozhranie SSH, prípadne cez konzolu Websupport.
- 9.4. Oprávnenosť a správnosť užívateľských prístupových práv je kontrolovaná automaticky, neoprávnené prístupy alebo prístupy s nepotvrdenou platnosťou sú rušené.
- 9.5. Pri dobe skončenia licencie na aplikáciu dlhšiu ako dva mesiace sú prístupy blokované k užívateľským dátam zrušené.
- 9.6. Užívateľské prístupy a všetky podstatné operácie sú v aplikácii zaznamenávané v auditnom zázname (Audit Log)
- 9.7. Každý užívateľ sa prihlasuje na vlastný účet. Zdieľanie účtu/prístupu s iným užívateľom je neprípustné a nie je podporované.
- 9.8. Je stanovená minimálna dĺžka hesla. Je vynucovaná zmena iniciačného hesla pri prvom. Nové heslo je vydávané len po overení identity užívateľa prostredníctvom prístupu k pracovnej emailovej schránke.
- 9.9. Dáta v neelektronickej podobe sú uchovávané a/alebo archivované len v trezoroch alebo uzamykateľných skrinách v rámci uzamykateľných priestorov.
- 9.10. Pri transportoch dát mimo internej siete Spracovateľa je doporučené použitie šifrovacích a autentizačných mechanizmov.

Conditions for personal data processing

pursuant to the provisions of Section 1746 (2) of Act No. 89/2012 Coll., the Civil Code, as amended, and pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) ("GDPR")

For the purposes of this document, **personal data** means any information relating to an identified or identifiable data subject. A data subject is considered to be determined or identifiable if he can be identified, directly or indirectly, in particular by number, code or one or more elements specific to his physical, physiological, mental, economic, cultural or social identity.

The **data subject** means the natural person to whom the personal data relates, i.e. users of the Schedy Service.

Any person who creates a user or company account is considered a **user of the Schedy Service**. The Schedy user declares that he is aware of his role as the **Personal Data Controller**, as well as the rights and obligations arising from this role. The user grants an explicit informed consent with this Data Processing Agreement (DPA).

The Processor of personal data is the company KMB group s.r.o., Piešťanská 3, 831 02 Bratislava, ID 47 425 288, a company registered in the Commercial Register kept at the District Court of Bratislava I, section Sro, insert 92152/B (hereinafter only the Company). The Company may entrust the management and processing of personal data to a third party for the purpose of operating and administering the Schedy Service.

1. Definition of processed personal data

1.1. Based on the Contract, the Processor processes personal data for the Controller to the following extent:

Purpose of processing	Scope of personal data	Special categories of personal data	Categories of data subjects
HR agenda management	Name and surname of a natural person; date of birth of natural person, sex, job position, internal employee number, workmobile and / or fixed telephone number; work email; photo; the date of joining the company, the date of leaving the company, the type of employment and the type of employment relationship.	no	employees
Management of the agenda of holidays	Dates of drawing on absence events (holidays, sick days, benefit days, etc. –	no	employees

and other types of absence	other events according to the system settings by the employer)		
Shift planning, work activity planning	Dates of work activities based on the definition of activities by the employer (e.g. work in the office, work at the client / customer, etc.)	no	employees
Employee attendance records	Records of the employee's hours worked within his working days.	no	employees
Administration of the employee's profile	In addition to the employee's identification data, the employee can also upload his / her images.	no	employees
User and application support	Data stored in the Schedy application	no	employees

1.2. The processor will process personal data in electronic form in accordance with this Agreement

1.3. The processor undertakes to process Personal Data with professional care.

2. Independence of the processor and instructions of the Controller

2.1. The Processor will process Personal Data separately in order to achieve the specified purpose of processing according to the Article 1.1. and, with the exercise of professional care, to independently decide on the execution of individual acts within the processing of personal data, which must be performed in accordance with the applicable legal regulations.

2.2. In the event that the Processor receives an instruction from the Controller, it is bound by it.

2.3. Instructions for the processing of personal data may be communicated on behalf of the Controller and accepted by the authorized person on behalf of the Processor, in written (electronic) form.

2.4. Processors are not bound by the Controller's instructions, which are:

2.4.1. made by a person other than the authorized person and addressed to a person other than the authorized person,

2.4.2. made in a form other than written (electronic),

2.4.3. contrary to the applicable law.

2.5. If any case arises where the Processor is not bound by the Controller's instruction, the Processor is obliged to inform the Controller of such a fact without undue delay.

3. Storage and security of personal data

- 3.1. The Processor undertakes to store and process Personal Data securely and to use all reasonable security systems and procedures suitable for the processing of Personal Data.
- 3.2. The Processor undertakes to prevent or take all possible steps to prevent unauthorized access, copying, modification, storage, reproduction, publication or distribution of Personal Data.
- 3.3. If the Processor uses the security elements in connection with the provision of the Services, it is obliged to maintain confidentiality about the security elements, it is not entitled to share them with third parties, transfer or otherwise misuse them.
- 3.4. The Processor creates backup copies of databases (weekly database backup), we save the last 4 backups. Restoration of data from the backup is charged at CZK 30,000.
- 3.5. In the event that either Party finds that:
 - 3.5.1. there has been an unauthorized or illegal processing of Personal Data;
 - 3.5.2. the Personal Data has been lost, damaged or destroyed or otherwise degraded;
 - 3.5.3. there has been a case of security breach;
 - 3.5.4. a third party has gained unauthorized access to any of the security features;it is obliged to notify the other Party without undue delay and to provide maximum co-operation for redress.
- 3.6. In providing quality Schedy Services, we are assisted by processors who work in accordance with European standards of personal data protection. The processing of personal data by these third parties is governed by their own terms of service.
- 3.7. Description of processing purposes:
 - 3.7.1. MailChimp and Mandrill Service for sending bulk messages and notifications.
MailChimp's personal data is transferred to the US, and MailChimp complies with EU-U.S. Privacy Shield.
 - 3.7.2. Google Analytics and Google Tag Manager statistics Services
(<https://policies.google.com/privacy/partners?hl=en>).

4. Declarations by Parties

- 4.1. The Processor declares and warrants to the Controller that
 - 4.1.1. fulfils all legal obligations arising for him from the GDPR and other legal regulations;
 - 4.1.2. will process personal data for the Controller for the entire duration of the Agreement in accordance with Czech law, in particular in accordance with the GDPR;
 - 4.1.3. will keep proper records of Personal Data processing activities within the meaning of Article 30 of the GDPR for the entire duration of the Agreement;
 - 4.1.4. will process only personal data in relation to defined data subjects in accordance with this Agreement to the extent and for the purpose specified by the Controller or in accordance with the purpose of this Agreement;
 - 4.1.5. will always process Personal Data on the basis of a valid legal ground, if it is a part of the Personal Data Collection Services by the Processor;

- 4.1.6. will process accurate Personal Data in accordance with this Agreement and will update it regularly. Personal data that are inaccurate with regard to the purposes for which they are processed shall be deleted or corrected by the Processor after the prior instruction of the Controller;
 - 4.1.7. will store Personal Data for the necessary time according to the Controller's Instruction. The processor undertakes to regularly check the deadlines for the liquidation of personal data and to ensure the liquidation of personal data, if the conditions are met;
 - 4.1.8. is able to guarantee that during the processing of personal data for the Controller it will not behave in such a way as to reduce the level of personal data protection ensured by this regulation.
- 4.2. The Controller declares and guarantees to the Processor that:
- 4.2.1. at the time of the transfer of Personal Data, the Personal Data is current and there is a valid legal title for their processing;
 - 4.2.2. is not aware of any risk of violation of valid legal regulations in connection with the current processing of Personal Data.
 - 4.2.3.** agrees to allow further processing of personal data by other processors who undertake to protect personal data to the minimum extent provided for in this contract. To the same extent as regards the purpose of processing and to the minimum extent as regards ensuring the security of the processing of personal data processes.

5. Cooperation

- 5.1. Co-operation in fulfilling the Controller's obligation to respond to requests for the exercise of data subjects' rights.
- 5.2. The Processor undertakes to provide the Controller with the necessary cooperation, which can be fairly requested, especially in the case of:
 - 5.2.1. implementation and maintenance of appropriate technical and organizational measures to secure personal data;
 - 5.2.2. security breach reporting;
 - 5.2.3. assessment of the impact of processing on the protection of personal data, if the Controller decides that an assessment of the impact of processing within the meaning of Article 35 of the GDPR is necessary;
 - 5.2.4. fulfilment of the obligations of prior consultation with the Office for Personal Data Protection within the meaning of Article 36 of the GDPR in the event of legal conditions.
- 5.3. At the request of the Controller, the Processor undertakes to provide, within a specified period of time, which may not be less than thirty (30) working days, the necessary information necessary to prove that the processing of personal data under the Contract is carried out in accordance with applicable law.
- 5.4. The Processor undertakes to allow the Controller and his representatives, at his request, within a reasonable period of time, which may not be less than thirty (30) working days:
 - 5.4.1. access to records on Personal Data processing activities;

5.4.2. check the technical and organizational security measures of the Personal Data;

6. Duration of processing

- 6.1. The Parties have agreed that the Processor will process personal data under this DPA for a definite period of time for the duration of the agreement on the use of the Schedy internet Service.
- 6.2. Upon termination of this Agreement, the Processor reserves the right to permanently delete the entire Controller's account, including all existing copies of personal data.

7. Confidentiality

- 7.1. The Contracting Parties declare that all data, information and facts related to this DPA and its performance and provision of Services under this DPA, in particular personal data processed under the DPA, including the content of the DPA (except information that is or becomes publicly known other than breach of this DPA and information held by the relevant party prior to its receipt from the other party) is confidential information ("Confidential Information"). The Parties undertake not to provide the Confidential Information to a third party and not to use it for any purpose other than the performance of this DPA, except:
 - 7.1.1. their advisers bound by professional secrecy to the same extent as the Parties, or
 - 7.1.2. the competent national and other administrative authorities and courts, where the parties are required by generally binding rules to provide them with this information, or
 - 7.1.3. information that is or becomes publicly available other than in violation of this DPA.
- 7.2. The Processor undertakes to bind its employees and other associates in a contractual relationship with the Processor who perform activities related to this DPA and its performance and provision of Services under this DPA.
- 7.3. The obligation of confidentiality under this DPA continues even after the termination of this DPA. The Parties are not entitled to disseminate or use confidential information within the meaning of this DPA in any way after the termination of the DPA or to enable their dissemination or use.

8. Issues related to personal data protection

- 8.1. If you have any questions or comments regarding the processing of the Company's personal data, please contact us.

Last update on 3/15/2021

9. List of technical and organizational measures taken to protect personal data

- 9.1. The application and user data are located on servers of Websupport company.
- 9.2. All accesses to the application are secured against eavesdropping using the https protocol and a valid encryption certificate.
- 9.3. Direct access to server administration is allowed only through the encrypted

SSH interface, or through the Websupport console.

- 9.4. The authorization and correctness of user access rights is checked automatically, unauthorized accesses or accesses with unconfirmed validity are cancelled.
- 9.5. If the application license expires for more than two months, access to the user data is blocked.
- 9.6. User accesses and all significant operations are recorded in the application in the audit log (AuditLog)
- 9.7. Each user logs in to their own account. Sharing an account / access with another user is not allowed and is not supported.
- 9.8. The minimum password length is set. The change of the initial password is forced at the first. The new password is issued only after verifying the user's identity through access to the work e-mail box.
- 9.9. Data in non-electronic form are stored and / or archived only in safes or lockable cabinets within lockable areas.
- 9.10. When transporting data outside the Processor's internal network, the use of encryption and authentication mechanisms is recommended.